The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/15/2020

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple products, the most severe of which could allow for arbitrary code execution.

- iCloud for Windows is a cloud storage service that can be used on Windows computers.
- watchOS is a mobile operating system created & developed by Apple to be utilized by its Apple Watch product line.
- iOS is a mobile operating system created & developed by Apple to be utilized by its mobile devices such as the iPhone.
- Safari is a web browser available for macOS.
- tvOS is an operating system based on iOS developed for AppleTV.
- macOS Server is a desktop operating system for Macintosh computers.
- iPadOS is a mobile operating system created & developed by Apple to be utilized by its iPad product line.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- watchOS versions prior to 7.2 and 6.3
- macOS versions prior to Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave
- tvOS versions prior to tvOS 14.3
- iOS versions prior to 14.3 and 12.5
- iPadOS versions prior to 14.3
- macOS Server versions prior to 5.11
- Safari versions prior to 14.0.2

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Apple products, the most severe of, which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

iOS 14.3 and iPadOS 14.3
- A logic issue was addressed with improved state management (CVE-2020-29613)
- An out-of-bounds write issue was addressed with improved bounds checking (CVE-2020-27948)
- An information disclosure issue was addressed with improved state management (CVE-2020-27946)
- A memory corruption issue existed in the processing of font files. This issue was addressed with improved input validation (CVE-2020-27943, CVE-2020-27944)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-29617, CVE-2020-29619)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-29618)
- An out-of-bounds write issue was addressed with improved bounds checking (CVE-2020-29611)
- Unauthorized code execution may lead to an authentication policy violation (CVE-2020-27951)
- A use after free issue was addressed with improved memory management (CVE-2020-15969)

iOS 12.5
- Unauthorized code execution may lead to an authentication policy violation (CVE-2020-27951)

watchOS 6.3
- Unauthorized code execution may lead to an authentication policy violation (CVE-2020-27951)

watchOS 7.2
- An out-of-bounds write issue was addressed with improved bounds checking (CVE-2020-27948)
- An information disclosure issue was addressed with improved state management (CVE-2020-27946)
- A memory corruption issue existed in the processing of font files. This issue was addressed with improved input validation (CVE-2020-27943, CVE-2020-27944)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-29617, CVE-2020-29619)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-29618)

- An out-of-bounds write issue was addressed with improved bounds checking (CVE-2020-29611)
- Unauthorized code execution may lead to an authentication policy violation (CVE-2020-27951)
- A use after free issue was addressed with improved memory management (CVE-2020-15969)

macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave

- A memory corruption issue was addressed with improved input validation (CVE-2020-27914, CVE-2020-27915)
- An application may be able to gain elevated privileges (CVE-2020-27903)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2020-27941)
- A malicious application may be able to bypass Privacy preferences (CVE-2020-29621)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-27910)
- An out-of-bounds read was addressed with improved bounds checking (CVE-2020-9943)
- An out-of-bounds read was addressed with improved bounds checking (CVE-2020-9944)
- An out-of-bounds write was addressed with improved input validation (CVE-2020-27916)
- Multiple integer overflows were addressed with improved input validation (CVE-2020-27906)
- An out-of-bounds write issue was addressed with improved bounds checking (CVE-2020-27948, CVE-2020-9955)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-9960, CVE-2020-27908)
- An out-of-bounds write was addressed with improved input validation (CVE-2020-10017)
- A logic issue was addressed with improved state management (CVE-2020-27922)
- An information disclosure issue was addressed with improved state management (CVE-2020-27946, CVE-2020-9849)
- A buffer overflow was addressed with improved size validation (CVE-2020-9962)
- An out-of-bounds write was addressed with improved input validation (CVE-2020-27952)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-9956)
- A memory corruption issue existed in the processing of font files (CVE-2020-27931, CVE-2020-27943, CVE-2020-27944)
- A logic issue was addressed with improved state management (CVE-2020-10002)
- A memory corruption issue was addressed with improved input validation (CVE-2020-27947)
- An out-of-bounds write issue was addressed with improved bounds checking (CVE-2020-29612)
- An attacker in a privileged network position may be able to unexpectedly alter application state (CVE-2020-9978)
- An out-of-bounds write was addressed with improved input validation (CVE-2020-27919)
- A memory corruption issue was addressed with improved input validation (CVE-2020-29616)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-27924, CVE-2020-29618)
- An out-of-bounds write issue was addressed with improved bounds checking (CVE-2020-29611)

- An out-of-bounds read was addressed with improved input validation (CVE-2020-29617, CVE-2020-29619)
- An out-of-bounds write was addressed with improved input validation (CVE-2020-27912, CVE-2020-27923)
- An out-of-bounds write issue was addressed with improved bounds checking (CVE-2020-10015, CVE-2020-27897)
- A memory corruption issue was addressed with improved memory handling (CVE-2020-27907)
- A logic issue was addressed with improved state management (CVE-2020-9974)
- A memory corruption issue was addressed with improved state management (CVE-2020-10016)
- Multiple memory corruption issues were addressed with improved input validation (CVE-2020-9967)
- A use after free issue was addressed with improved memory management (CVE-2020-9975, CVE-2020-27899)
- A race condition was addressed with improved state handling (CVE-2020-27921)
- A malicious application may cause unexpected changes in memory belonging to processes traced by DTrace (CVE-2020-27949)
- A malicious application may be able to elevate privileges (CVE-2020-29620)
- An integer overflow was addressed through improved input validation (CVE-2020-27911)
- A use after free issue was addressed with improved memory management (CVE-2020-27920)
- A use after free issue was addressed with improved memory management (CVE-2020-27926)
- A parsing issue in the handling of directory paths was addressed with improved path validation (CVE-2020-10014)
- A path handling issue was addressed with improved validation (CVE-2020-10010)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-13524)
- A logic issue was addressed with improved state management (CVE-2020-10004)
- A logic issue was addressed with improved restrictions (CVE-2020-27901, CVE-2020-10008)
- A logic issue was addressed with improved state management (CVE-2020-10007)
- An access issue was addressed with improved access restrictions (CVE-2020-10012)
- A path handling issue was addressed with improved validation (CVE-2020-27896)
- A logic issue was addressed with improved state management (CVE-2020-10009)
- A use after free issue was addressed with improved memory management (CVE-2020-15969)
- A denial of service issue was addressed with improved state handling (CVE-2020-27898)
- A logic issue was addressed with improved validation (CVE-2020-9971)
- An issue existed in the handling of snapshots. The issue was resolved with improved permissions logic (CVE-2020-27900)
- The issue was addressed with improved handling of icon caches (CVE-2020-9963)
- A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement (CVE-2020-9977)
- An inconsistent user interface issue was addressed with improved state management (CVE-2020-9942)
- This issue was addressed with improved checks (CVE-2020-9991)
- This issue was addressed with improved entitlements (CVE-2020-10006)

macOS Server 5.11

- An issue existed in the parsing of URLs. This issue was addressed with improved input validation (CVE-2020-9995)

tvOS 14.3

- An out-of-bounds write issue was addressed with improved bounds checking (CVE-2020-27948)
- An information disclosure issue was addressed with improved state management (CVE-2020-27946)
- A memory corruption issue existed in the processing of font files. This issue was addressed with improved input validation (CVE-2020-27943, CVE-2020-27944)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-29617, CVE-2020-29619)
- An out-of-bounds read was addressed with improved input validation (CVE-2020-29618)
- An out-of-bounds write issue was addressed with improved bounds checking (CVE-2020-29611)
- A use after free issue was addressed with improved memory management (CVE-2020-15969)

Safari 14.0.2

- A use after free issue was addressed with improved memory management (CVE-2020-15969)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Apple:

https://support.apple.com/en-us/HT212003
https://support.apple.com/en-us/HT212004
https://support.apple.com/en-us/HT212005
https://support.apple.com/en-us/HT212006
https://support.apple.com/en-us/HT212007
https://support.apple.com/en-us/HT212009

https://support.apple.com/en-us/HT212011
https://support.apple.com/en-us/HT211932
https://support.apple.com/en-us/HT211931

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9943
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9944
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9962
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9967
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9974
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9975
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9978
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9995
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10002
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10004
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10009
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13524
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15969
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27896
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27897
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27898
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27901
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27903
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27906
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27907
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27908
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27910
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27911
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27912
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27914
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27915
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27916
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27919
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27920
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27921
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27922
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27923
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27924
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27926
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27931
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27941
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27943

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27944
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27946
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27947
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27948
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27949
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27952
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29611
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29612
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29613
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29616
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29617
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29618
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29619
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29620
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29621
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9955
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27900
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9977
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9942
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9849
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27899
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10006